Min Jia
Zheng/China/IBM@IBMCN

02/06/2006 10:01 PM
This document expires on 05/08/2006

To Jennifer Smith/Washington/IBM@IBMUS
cc Yan SD Zhang/China/IBM@IBMCN, Su Sha Zhang/China/IBM@IBMCN
bcc
Subject Fw: Your 09/08/2005 Information Disclosure Statement For FR9-2002-0060CN1

Hello Jennifer,

Here is the english abstract of CN 1314754A

"Methods, systems and computer program products are provided which provide profile information associated with a client to a server by generating, at the client, a profile document containing profile information associated with the client and incorporating in the profile document a designator which indicates that profile information identified by the designator is not provided by the client and is provided by a network intermediary in a path between the client and the server. The designator in the profile document is encrypted utilizing a key associated with the client and the profile document with the encrypted designator transmitted from the client to the server utilizing the path. Method, systems and computer program products corresponding to the network intermediaries are also provided."

It is a family patent of **US6978373** B1. You can find the English specification in the following website.
http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=CN1314754&F=0

Best Regards,

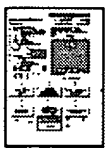
Zheng Minjia (郑闽迦)
IP Professional
Intellectual Property Law
IBM China Company Limited
Building 19, Zhongguancun Software Park, 8 Dongbeiwang West Road, Haidian District, 100094,
Beijing P.R.C.

Tel:86-10-58748463

The Delphion Integrated View: INPADOC Record

Title: **CN1314754A: METHOD AND SYSTEM FOR COMPLETING CUSTERMER MACHINE FILE BY NETWORK INTERMEDIATE BODY**

Derwent Title: Client profile information provision in client-server system, involves transmitting profile document with encrypted designator, indicating that profile information is provided by network intermediary, to server [Derwent Record]



High Resolution

Country: **CN** China

Kind: **A** Unexamined APPLIC. open to Public inspection

Inventor: **STEFFEN GEORGE SCHELD**; United States of America
SANDIP JISAN XINHOL; United States of America

Assignee: **INTERNATIONAL BUSINESS MACHINE CORP.** United States of America
News, Profiles, Stocks and More about this company

Published / Filed: **2001-09-26** / 2001-03-21

Application Number: **CN2001000111846**

IPC Code: IPC-7: **H04L 12/22;**

ECLA Code: None

Priority Number: 2000-03-22 **US2000000533644**

INPADOC Legal Status: None **Get Now:** Family Legal Status Report

Family:

PDF	Publication	Pub. Date	Filed	Title
	US6978373	2005-12-20	2000-03-22	Methods systems and computer program products for providing secure client profile completion by network intermediaries
☑	JP2001282649A2	2001-10-12	2001-02-21	METHOD AND SYSTEM FOR PROVIDING PROFILE INFORMATION OF CLIENT FOR SERVER
☑	JP03661776B2	2005-06-22	2001-02-21	
☑	GB2366166B2	2003-12-31	2001-03-21	Methods, systems and computer program products for providing secure client profile completion by network intermediaries
	GB2366166A1	2002-02-27		
	GB2366166A	2002-02-27	2001-03-21	METHODS, SYSTEMS AND COMPUTER PRODUCTS FOR PROVIDING SECURE CLIENT PROFILE COMPLETION BY NETWORK INTERMEDIARIES
	GB0107025A0	2001-05-09		
☑	GB0107025A	2001-05-09	2001-03-21	METHODS SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING SECURE CLIENT PROFILE COMPLETION BY NETWORK INTERMEDIARIES
				METHOD AND SYSTEM FOR COMPLETING

☑	CN1314754A	2001-09-26	2001-03-21	CUSTERMER MACHINE FILE BY NETWORK INTERMEDIATE BODY
9 family members shown above				

Other Abstract Info: None

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 12/22

[12]发明专利申请公开说明书

[21]申请号 01111846.6

[43]公开日 2001年9月26日

[11]公开号 CN 1314754A

[22]申请日 2001.3.21 [21]申请号 01111846.6
[30]优先权
[32]2000.3.22 [33]US [31]09/533,644
[71]申请人 国际商业机器公司
地址 美国纽约
[72]发明人 斯蒂芬·乔治·希尔德
桑蒂普·基山·星霍尔

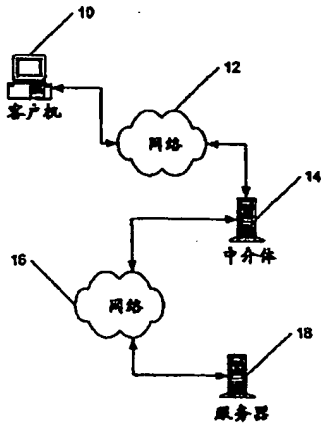
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 于 静

权利要求书9页 说明书11页 附图页数5页

[54]发明名称 由网络中介体完成安全的客户机档案的方法和系统

[57]摘要

提供了方法、系统和计算机程序产品，它们在客户机处产生一个 含有与该客户机关联的档案信息的档案文件并在该档案文件中纳入一 个指示器，该指示器指出由该指示器标识的档案信息不是由客户机提 供的而是由该客户机和服务器之间路径中的一个网络中介体提供的，从而向服务器提供与该客户机关联的档案信息。利用与该客户机关联 的密钥对档案文件中的指示器加密，并利用该路径将带有加密指示器 的档案文件从客户机发送给服务器。



ISSN1008-4274

权 利 要 求 书

1.一种向服务器提供与客户机关联的档案信息的方法，该方法包含下列步骤:

在客户机处产生含有与该客户机关联的档案信息的档案文件;

在该档案文件中纳入一个指示器，它指出由该指示器标识的档案信息不是由该客户机提供，而是由该客户机和服务器之间路径上的一个网络中介体提供; 以及

利用该路径从客户机向服务器发送带有该指示器的档案文件.

2.根据权利要求 1 的方法，其中被纳入档案文件的指示器包含一个档案信息标识和一个与档案信息标识关联的通配符指示器，该档案信息标识标明该档案文件中的档案信息类型，该通配符指示器指出，与该档案信息标识关联的该类型档案信息是由该客户机和服务器之间路径中的网络中介体提供的。

3.根据权利要求 1 的方法，进一步包含利用与该客户机关联的密钥对档案文件中的指示器加密的步骤。

4.根据权利要求 3 的方法，其中对指示器加密的步骤包含利用与该客户机关联的私人密钥对通配符指示器加密以提供加密的指示器的步骤.

5.根据权利要求 4 的方法，其中该通配符指示器包含一个与该客户机关联的客户机标识、一个令牌和一个加密的值，其中对通配符指示器加密的步骤包含对令牌加密从而提供加密的值的步骤。

6.根据权利要求 5 的方法，其中对令牌加密的步骤进一步包含对令牌和一预先定义的字符串加密的步骤。

7.根据权利要求5的方法，其中的令牌是一个随机产生的值。

8.根据权利要求 3 的方法，其中对指示器加密的步骤包含利用与该客户机关联的私人密钥对通配符指示器和档案信息标识进行加密以提供加密的指示器的步骤.

9.根据权利要求 8 的方法，其中该通配符指示器包含一个与该客

户机关联的客户机标识、一个令牌和一个加密的值，其中对通配符指示器和档案信息标识进行加密的步骤包含对该令牌和档案信息标识加密以提供加密的值的步骤.

10.根据权利要求 8 的方法，其中对令牌和档案信息标识加密的步骤进一步包含对该令牌、档案信息标识及一预先定义的字符串进行加密的步骤.

11.根据权利要求 10 的方法，其中的令牌是一个随机产生的值.

12.根据权利要求 1 的方法，进一步包含利用该网络中介体的公共密钥对指示器加密的步骤.

13.根据权利要求 3 的方法，进一步包含下列步骤:

在网络中介体处接收由客户机发送的档案文件；以及

其中网络中介体进行下列步骤;

如果在该档案文件中纳入的指示器被加密，则对该档案文件中纳入的该指示器解密;

如果该网络中介体具有可得到的由指示器标识的档案信息，则把该指示器标识的档案信息纳入档案文件以提供一个修改过的档案文件;

向服务器发送该修改过的档案文件.

14.一种向服务器提供客户机档案信息的方法，该方法包含下列步骤:

在网络中介体处接收来自客户机的档案文件供传送给服务器;

确定该档案文件是否有一部分被加密;

对该档案文件的加密部分解密;

解析该档案文件的被解密部分，以确定是否在该档案文件的解密部分中提供了一个指示器，它指明由该指示器标明的档案信息要由该网络中介体纳入到该档案文件中;

将标明的档案信息纳入档案文件，从而提供一个修改过的档案文件；以及

把修改过的档案文件发送给服务器.

15.根据权利要求 14 的方法，其中被纳入档案文件的指示器包含一个档案信息标识和一个与档案信息标识关联的通配符指示器，该档案信息标识标明该档案文件中的档案信息类型，该通配符指示器指出与档案信息标识关联的该类型档案信息是由该客户机和服务器之间路径中的网络中介体提供的.

16.根据权利要求 15 的方法，其中对指示器解密的步骤包含利用与该客户机关联的私人密钥对文件档案的加密部分解密以提供指示器的步骤.

17.根据权利要求 16 的方法，其中的通配符指示器包含一个与该客户机关联的客户机标识、一个令牌和一个加密的值，其中对该文件档案加密部分解密的步骤包含对加密的值解密的步骤。

18.根据权利要求 16 的方法，其中该令牌是一个随机产生的值。

19.根据权利要求 15 的方法，其中对文件档案加密部分进行解密的步骤包含下列步骤:

对档案文件的加密部分解密，以提供一通配符指示器；以及

利用与该客户机关联的私人密钥对档案信息标识解密，以提供解密的指示器.

20.根据权利要求 14 的方法，进一步包含利用网络中介体的私人密钥对文件档案的加密部分进行解密的步骤.

21.一种向服务器提供与客户机关联的档案信息的系统，包含:

在客户机处产生含有与该客户机关联的档案信息的档案文件的装置;

在该档案文件中纳入一个指示器的装置，该指示器指出由该指示器标识的档案信息不是由该客户机提供，而是由该客户机和服务器之间路径上的一个网络中介体提供；以及

利用该路径从客户机向服务器发送带有该指示器的档案文件的装置。

22.根据权利要求 21 的系统，其中被纳入档案文件的指示器包含一个档案信息标识和一个与档案信息标识关联的通配符指示器，该档

案信息标识标明该档案文件中的档案信息类型，该通配符指示器指出，与该档案信息标识关联的该类型档案信息是由该客户机和服务器之间路径中的网络中介体提供的.

23.根据权利要求 21 的系统，进一步包含利用与该客户机关联的密钥对档案文件中的指示器加密的装置.

24.根据权利要求 23 的系统，其中对指示器加密的装置包含利用与该客户机关联的私人密钥对通配符指示器加密以提供加密的指示器的装置.

25.根据权利要求 24 的系统，其中该通配符指示器包含一个与该客户机关联的客户机标识、一个令牌和一个加密的值，其中对通配符指示器加密的装置包含对令牌加密从而提供加密的值的装置.

26.根据权利要求 25 的系统，其中对令牌加密的装置进一步包含对令牌和一预先定义的字符串加密的装置.

27.根据权利要求25的系统，其中该令牌是一个随机产生的值.

28.根据权利要求 23 的系统，其中对指示器加密的装置包含利用与该客户机关联的私人密钥对通配符指示器和档案信息标识进行加密以提供加密的指示器的装置.

29.根据权利要求 28 的系统，其中该通配符指示器包含一个与该客户机关联的客户机标识、一个令牌和一个加密的值，其中对通配符指示器和档案信息标识进行加密的装置包含对该令牌和档案信息标识加密以提供加密的值的装置.

30.根据权利要求 28 的系统，其中对令牌和档案信息标识加密的装置进一步包含对该令牌、档案信息标识及一预先定义的字符串进行加密的装置.

31.根据权利要求30的系统，其中该令牌是一个随机产生的值.

32.根据权利要求 21 的系统，进一步包含利用该网络中介体的公共密钥对指示器加密的装置.

33.根据权利要求21的系统，进一步包含:

在网络中介体处接收由客户机发送的档案文件的装置;

如果在该档案文件中纳入的指示器被加密则对该指示器解密的装置;

把该指示器标识的档案信息纳入档案文件以提供一个修改过的档案文件的装置;

向服务器发送该修改过的档案文件的装置.

34.一种向服务器提供客户机档案信息的系统，包含:

在网络中介体处接收来自客户机的档案文件供传送给服务器的装置;

确定该档案文件是否有一部分被加密的装置;

对该档案文件的加密部分解密的装置;

解析该档案文件的被解密部分，以确定是否在该档案文件的解密部分中提供了一个指示器的装置，该指示器指明由该指示器标明的档案信息要由该网络中介体纳入到该档案文件中;

将标明的档案信息纳入档案文件，从而提供一个修改过的档案文件的装置；以及

把修改过的档案文件发送给服务器的装置.

35.根据权利要求 34 的系统，其中被纳入档案文件的指示器包含一个档案信息标识和一个与档案信息标识关联的通配符指示器，该档案信息标识标明该档案文件中的档案信息类型，该通配符指示器指出与该档案信息标识关联的该类型档案信息是由网络中介体提供的.

36.根据权利要求 35 的系统，其中对指示器解密的装置包含利用与该客户机关联的私人密钥对文件档案的加密部分解密以提供指示器的装置.

37.根据权利要求 36 的系统，其中的通配符指示器包含一个与该客户机关联的标识、一个令牌和一个加密的值，其中对该文件档案加密部分解密的装置包含对加密的值解密的装置.

38.根据权利要求36的系统，其中该令牌是一个随机产生的值.

39.根据权利要求 35 的系统，其中对文件档案加密部分进行解密的装置包含:

对档案文件的加密部分解密，以提供一通配符指示器的装置；以及

利用与该客户机关联的私人密钥对档案信息标识解密，以提供解密的指示器的装置.

40.根据权利要求 34 的系统，进一步包含利用网络中介体的私人密钥对文件档案的加密部分进行解密的装置.

41.一种向服务器提供与客户机关联的档案信息的计算机程序产品，包含:

计算机可读的存储介质，它有计算机可读程序代码包含在该介质中，所述计算机可读程序代码包含:

在客户机处产生含有与该客户机关联的档案信息的档案文件的计算机可读程序代码;

在该档案文件中纳入一个指示器的计算机可读程序代码，该指示器指出由该指示器标识的档案信息不是由该客户机提供，而是由该客户机和服务器之间路径上的一个网络中介体提供；以及

利用该路径从客户机向服务器发送带有该指示器的档案文件的计算机可读程序代码.

42.根据权利要求 41 的计算机程序产品，其中被纳入档案文件的指示器包含一个档案信息标识和一个与档案信息标识关联的通配符指示器，该档案信息标识标明该档案文件中的档案信息类型，该通配符指示器指出，与该档案信息标识关联的该类型档案信息是由该客户机和服务器之间路径中的网络中介体提供的.

43.根据权利要求 41 的计算机程序产品，进一步包含利用与该客户机关联的密钥对档案文件中的指示器加密的计算机可读程序代码.

44.根据权利要求 43 的计算机程序产品，其中对指示器加密的计算机可读程序代码包含利用与该客户机关联的私人密钥对通配符指示器加密以提供加密的指示器的计算机可读程序代码.

45.根据权利要求 44 的计算机程序产品，其中该通配符指示器包含一个与该客户机关联的客户机标识、一个令牌和一个加密的值，其

中对通配符指示器加密的计算机可读程序代码包含对令牌加密从而提供加密的值的计算机可读程序代码.

46.根据权利要求 45 的计算机程序产品，其中对令牌加密的计算机可读程序代码进一步包含对令牌和一个预先定义的字符串加密的计算机可读程序代码.

47.根据权利要求 45 的计算机程序产品，其中该令牌是一个随机产生的值.

48.根据权利要求 43 的计算机程序产品，其中对指示器加密的计算机可读程序代码包含利用与该客户机关联的私人密钥对通配符指示器和档案信息标识进行加密以提供加密的指示器的计算机可读程序代码.

49.根据权利要求 48 的计算机程序产品，其中该通配符指示器包含一个与该客户机关联的客户机标识、一个令牌和一个加密的值，其中对通配符指示器和档案信息标识进行加密的计算机可读程序代码包含对该令牌和档案信息标识加密以提供加密的值的计算机可读程序代码。

50.根据权利要求 48 的计算机程序产品，其中对令牌和档案信息标识加密的计算机可读程序代码进一步包含对该令牌、档案信息标识及一预先定义的字符串进行加密的计算机可读程序代码.

51.根据权利要求 49 的计算机程序产品，其中该令牌是一个随机产生的值.

52.根据权利要求 41 的计算机程序产品，进一步包含利用该网络中介体的公共密钥对指示器加密的计算机可读程序代码.

53.根据权利要求 41 的计算机程序产品，进一步包含:

在网络中介体处接收由客户机发送的档案文件的计算机可读程序代码;

如果在该档案文件中纳入的指示器被加密，则对该指示器解密的计算机可读程序代码;

把该指示器标识的档案信息纳入档案文件以提供一个修改过的档

案文件的计算机可读程序代码;

向服务器发送该修改过的档案文件的计算机可读程序代码.

54.一种向服务器提供客户机档案信息的计算机程序产品，包含:

计算机可读的存储介质，它有计算机可读程序代码包含在该介质中，所述计算机可读程序代码包含:

在网络中介体处接收来自客户机的档案文件供发送给服务器的计算机可读程序代码;

确定该档案文件是否有一部分被加密的计算机可读程序代码;

对该档案文件的加密部分解密的计算机可读程序代码;

解析该档案文件的被解密部分，以确定是否在该档案文件的解密部分中提供了一个指示器的计算机可读程序代码，该指示器指明由该指示器标明的档案信息要由该网络中介体纳入到该档案文件中;

将标明的档案信息纳入档案文件，从而提供一个修改过的档案文件的计算机可读程序代码; 以及

把修改过的档案文件发送给服务器的计算机可读程序代码。

55.根据权利要求 54 的计算机程序产品，其中被纳入档案文件的指示器包含一个档案信息标识和一个与档案信息标识关联的通配符指示器，该档案信息标识标明该档案文件中的档案信息类型，该通配符指示器指出与该档案信息标识关联的该类型档案信息是由网络中介体提供的.

56.根据权利要求 55 的计算机程序产品，其中对指示器解密的计算机可读程序代码包含利用与该客户机关联的私人密钥对文件档案的加密部分解密以提供指示器的计算机可读程序代码.

57.根据权利要求 56 的计算机程序产品，其中的通配符指示器包含一个与该客户机关联的标识、一个令牌和一个加密的值，其中对该文件档案加密部分解密的计算机可读程序代码包含对加密的值解密的计算机可读程序代码。

58.根据权利要求 56 的计算机程序产品，其中该令牌是一个随机产生的值。

59.根据权利要求 55 的计算机程序产品，其中对文件档案加密部分进行解密的计算机可读程序代码包含:

对档案文件的加密部分解密，以提供一通配符指示器的计算机可读程序代码；以及

利用与该客户机关联的私人密钥对档案信息标识解密，以提供解密的指示器的计算机可读程序代码.

60.根据权利要求 54 的计算机程序产品，进一步包含利用网络中介体的私人密钥对文件档案的加密部分进行解密的计算机可读程序代码。

说　　明　　书

由网络中介体完成安全的客户机档案的方法和系统

本发明涉及客户档案，更具体地说，涉及客户档案信息的安全性。

随着服务器提供给客户机的定制信息的增加，从客户机传送给服务器的客户机信息也已增加。服务器除了在其他方面使用客户机信息外，可能用客户机信息来改制向客户机提供的内容。例如，如果向服务器报告了一客户机的位置，那么服务器可根据客户机的位置向该客户机提供内容。类似地，如果客户机向服务器通告了它所连接的网络，那么服务器可以利用该信息向客户机提供针对该网络的信息。

作为一例，如果一个移动客户机连到美国北卡罗莱那的研究三角形公园(Research Triangle Park)中的一个网络，那么如果该客户机向服务器提供的档案信息指明它的位置是在北卡罗莱那，那么该服务器便可能向该客户机提供关于北卡罗莱那的信息。然后，如果该客户机后来通过日本东京中的一个网络连到该服务器，而且该客户机向该服务器提供的档案信息指明它的位置是在东京，那么该服务器可以向该客户机提供关于东京的信息。

存在各种方法使客户机可以向服务器通告它的偏好和能力。例如，信息可以嵌入超文本传输协议（HTTP）用户代理字段，或者它可以嵌入一个统一资源定位器（URL）本身之中。正在出现的标准，如W3C组合能力/偏好档案(CC/PP)标准和WAP Forum的用户代理档案标准，类似地定义了格式，利用这些格式可由客户机把信息嵌入HTTP请求之中。

然而，服务器支持这种能力可能需要的信息并不总是客户机能实际得到的。例如，客户机可能没有要提供给服务器的位置信息。如果客户机没有与一全球定位系统（GPS）相关联，便可能发生这种情况。所以，客户机可能不能靠它本身向服务器提供这种位置信息。然而，

一个网络中介体，即在客户机和服务器之间路径中的一个数据处理系统可能会得到这种信息。尽管网络中介体可能具有这种信息，但网络中介体可能需要得到通知，即通知它应把这种信息作为该客户机档案的一部分传送给服务器。然而，法律考虑可能阻止一个网络中介体（如服务提供者）在未经最终用户明确允许的情况下向第三服务方提供这种信息。这样，可能需要客户机明确地通知网络中介体把它的位置信息传送给该服务器。

当网络中介体代表一客户机提供信息时可能产生的一个问题是安全性。因为信息不是由客户机直接提供的，所以可能必须确定这种信息的真实性和保证该信息不是由伪装成该客户的某人所提供。然而，保密协议，如用于保密偏好方案的平台（P3P）是在客户机和服务器之间端到端操作的，可能不适于向网络中介体提供授权以向服务器提供关于客户机的信息。于是，在如何向服务器提供客户机档案信息的安全性方面需要改进。

本发明的实施例包括向服务器提供与一客户机相关联的档案信息的方法、系统和计算机程序产品，这是通过在客户机处产生一个档案文件，该档案文件包含与该客户机关联的档案信息，并在该档案文件中纳入一个指示器，它指示由该指示器标识的档案信息不是由该客户机提供的，而是由客户机和服务器之间的路径中的网络中介体提供的。利用与该客户机关联的密钥对档案文件中的指示器加密，并利用该路径将带有加密指示器的档案文件从客户机传送到服务器。

在本发明的具体实施例中，纳入档案文件的指示器包含一个档案信息标识和一个与档案信息标识关联的通配符指示器，该档案信息标识标明档案文件中的档案信息类型，该通配符指示器指出与该档案信息标识相关联的该类型档案信息是由客户机和服务器之间路径中的网络中介体提供。再有，可以利用与该客户机关联的私人密钥对通配符指示器加密来提供加密的指示器，从而提供对指示器的加密。

在本发明的另一些实施例中，通配符指示器包含一个与客户机关联的客户标识、一个令牌和一个加密的值。在每个实施例中，可以通

过对令牌加密从而提供加密的值来实现对通配符指示器的加密。另一种作法是，可对该令牌和一个预先定义的字符串加密。该令牌可以是一个随机产生的值。

在本发明的又一些实施例中，可以利用与该客户机关联的私人密钥对通配符指示器和档案信息标识进行加密来对指示器加密，从而提供加密的指示器。在这些实施例中，通配符指示器可以是一个与该客户机关联的客户机标识、一个令牌和一个加密的值。然后，可以通过对令牌和档案信息标识加密从而提供加密的值来实现对通配符指示器和档案信息标识的加密。再有，可以通过对令牌、档案信息标识和一个预先定义的字符串加密来提供对令牌和档案信息标识的加密。在本发明的又一实施例中，利用该网络中介体的公共密钥对指示器加密。

在本发明的其他实施例中，由客户机传送的档案文件在网络中介体处被接收。该网络中介体对所收到的档案文件中的指示器解密，把指示器标识的档案信息纳入该档案文件，以提供修改过的档案文件并把修改过的档案文件传送给服务器。

在本发明的另一些实施例中，方法、系统和计算机程序产品，可通过在网络中介体接收来自客户机的档案文件供传送给服务器，来向服务器提供客户机档案信息。网络中介体确定是否有一部分档案文件被加密并对档案文件中加密的部分解密。对档案文件的解密部分进行解析，以确定是否在该档案文件的解密部分中提供了一个指示器，该指示器指出，由该指示器标识的档案信息要由该网络中介体纳入到档案文件中。如果是这样，则网络中介体将所标识的档案信息纳入到该档案文件中，从而提供一个修改过的档案文件并把修改过的档案文件传送给服务器。

在又一些实施例中，被纳入档案文件的指示器包含一个档案信息标识和一个与该档案信息标识关联的通配符指示器，前者标识档案文件中的档案信息类型，后者指出与档案信息标识关联的该类型档案信息是由网络中介体提供的。在另一些实施例中，可以利用提供给指示器的与该客户机关联的私人密钥来对文件档案的加密部分解密，从而

实现对指示器的解密.

在又一些实施例中，通配符指示器可以是一个与客户机关联的客户机标识、一个令牌和一个加密的值. 在这种情况中，可通过对加密值解密来对文件档案的加密部分解密. 再有，该令牌可以是一个随机产生的值.

在本发明的又一些实施例中，可利用与该客户机关联的私人密钥来对文件档案的加密部分解密以提供通配符指示器和档案文件标识，从而实现对档案文件加密部分的解密，以提供解密的指示器.

再有，文件档案的加密部分还可利用网络中介体的私人密钥来解密.

尽管上面对本发明的描述主要是针对本发明的方法方面，但也提供了系统和/或计算机程序产品二者.

图 1 是根据本发明实施例的客户机－服务器系统框图;

图 2 是根据本发明实施例的数据处理系统框图;

图 3 是根据本发明实施例的数据处理系统的更详细的框图;

图 4 是根据本发明实施例说明客户机操作的流程图;

图 5 是根据本发明实施例说明网络中介体操作的流程图.

下文中将参考显示本发明最佳实施例的附图，更充分地描述本发明. 然而，本发明可以以许多不同的形式实现，不应被认作是局限于这里提出的实施例; 相反，提供这些实施例从而使本说明详尽和完全，并将向本领域技术人员充分传达本发明的范围.

如本领域技术人员将会理解的那样，本发明可以作为方法、数据处理系统或计算机程序产品来实现. 因此，本发明可以采取完全硬件实现、完全软件实现或把软件和硬件方面组合起来实现的形式. 再有，本发明可采取计算机可用存储介质上的计算机程序产品的形式，该计算机可用存储介质具有计算机可用程序代码装置，可以利用任何适当的计算机可读介质，包括硬盘、CD－ROM、光存储装置或磁存储装置.

实现本发明操作的计算机程序代码可以以面向对象的程序设计语

言写成，如 Java®、Smalltalk 或 C++．然而，实现本发明操作的计算机程序代码还可以以传统的过程编程语言写成，如“C“编程语言．该程序代码可以作为独立的软件包完全在用户计算机上执行、部分地在用户计算机上执行；部分地在用户计算机上和部分地在远程计算机上执行，或者完全在远程计算机上执行．在后面的这种情况中，远程计算机可通过局域网（LAN）或广域网（WAN）与用户计算机相连，或者可以是与一外部计算机相连（例如使用因特网服务提供者通过因特网相连）．

下面将参考根据本发明一个实施例的方法、装置（系统）和计算机程序产品的流程图和/或方框图来描述本发明．将会理解，流程图和/或方框图的每一块，以及流程图和/或方框图中一些块的组合，可以由计算机程序指令来实现．这些计算机程序指令可以提供给一通用计算机、专用计算机或其他可编程数据处理装置的处理器，以产生一个机器，从而由该计算机或其他可编程数据处理装置的处理器执行的指令建立一种装置，以实现流程图和/或方框图的一个或多个块中指定的功能．

这些计算机程序指令还可以存储在计算机可读存储器中，它能指引一计算机或其他可编程数据处理装置以一特定的方式发挥功能，从而使计算机可读存储器中存储的指令产生一个包括指令装置的制成品，这种装置实现流程图和/或方框图的一个或多个块中指定的功能．

还可以将计算机程序指令装入到计算机或其他可编程数据处理装置，以使一系列操作步骤可以在计算机或其他可编程数据处理装置上执行，从而产生由计算机实施的过程，从而在计算机或其他可编程装置上执行的指令提供了步骤，实现了流程图或方框图的一个块或多个块中指定的功能．

如在下文中更详细描述的那样，本发明提供由网络中介体产生档案信息的安全性．这种安全性是通过对客户档案文件中的信息加密来提供的，该信息指定该网络中介体要提供客户档案信息．本发明的实施例可以用在例如如下美国专利申请中描述的那些系统中，该申请与

本申请同时提交和共同转让，题为“指定所需装置属性供嵌入万维网文件请求中的方法和系统“，代理人文档号 RSW9－99－132，该申请披露的内容纳入这里作为参考，如同在这里完全提出一样。

现在将参考图 1 至图 5 描述本发明的各种实施例。图 1 显示在其中可利用本发明实施例的网络环境。如图 1 中所见，一个客户和数据处理系统 10，如个人计算机、膝上计算机、盛行的计算装置（如个人数字助理(PDA)、智能电话、或其他移动终端），在网络 16 上与作为服务器 18 的另一数据处理系统通信。在客户机 10 和服务器 18 之间的通信中，可以有一个数据处理系统作为网络中介体 14，它接收来自客户机 10 的消息并把消息传送给服务器 18。这种网络中介体 14 的实例包括代理服务器、网关服务器或服务提供器，然而，如这里使用的术语那样，从客户机 10 接收消息并把消息传送给服务器 18 的任何数据处理系统都可认为是网络中介体。

现在参考图 2，根据本发明实施例的数据处理系统 230 的一个实施示例通常包括输入装置 232，（如键盘或小键盘）、显示器 234、以及与处理器 238 通信的存储器 236。数据处理系统 230 可以进一步包括扬声器 244 和 I/O 数据端口 246，它也与处理器 238 通信。I/O 数据端口 246 可用于该数据处理系统 230 和另一计算机系统或一网络（例如因特网）之间的通信。这些部件可以是传统的部件，如在许多传统的盛行的计算装置中使用的那些部件，它们可配置成如这里所述那样操作。再有，如本领域技术人员将会理解的那样。数据处理系统 230 可被配置成客户机 10、网络中介体 14 或服务器 18。

图 3 是数据处理系统实施例的方框图，它说明根据本发明的系统、方法和计算机程序产品。处理器 238 经由地址/数据总线 248 与存储器 236 通信。处理器 238 可以是任何市场可得到的或定制的微处理器。存储器 236 是包含软件和数据的存储器装置总体体系结构的代表，这些软件和数据用于实现数据处理系统 230 的功能。存储器 236 可包括（但不限于）如下类型的装置：高速缓存、ROM、PROM、EPROM、EEPROM、闪速存储器、SRAM 和 DRAM。

如图 3 中所示，存储器 236 可以包括用于数据处理系统 230 的若干类型软件和数据：操作系统 252；应用程序 254；输入/输出（I/O）装置驱动器 258；以及数据 256。如本领域技术人员将会理解的那样，操作系统 252 可以是适于数据处理系统使用的任何操作系统，如 OS/2、AIX 或系统 390（这些来自国际商用机器公司(IBM), Armonk, Ny），Windows 95、Windows 98 或 Windows 2000（这些来自微软公司，Redmond, WA），Unix 或 Linux。I/O 装置驱动器 258 通常包括由应用程序 254 通过操作系统 252 访问的软件例行程序，用于与输入装置 232、显示器 234、扬声器 244、I/O 数据端口 246、以及某些存储器 236 部件等装置进行通信。应用程序 254 是实现数据处理系统 230 的各种特性的程序的例证，而且最好包括至少一个可以利用本发明实施例的安全档案方面的应用程序。最后，数据 256 代表应用程序 254、操作系统 252、I/O 装置驱动器 258、以及其他可驻留在存储器 236 中的其他软件程序所使用的静态和动态数据。

如在图 3 中还可看到的那样，应用程序 254 最好包括一个客户机档案模块 260。客户机档案模块 260 最好进行如这里描述的操作，以提供来自网络中介体的安全档案信息。就此而论，客户机档案模块可以是不同的，取决于图 3 中所示系统是客户机 10 还是网络中介体 14。另一种作法是，单一的客户机档案模块 260 可以被用于客户机 10 和网络中介体 14 二者。再有，存储器 236 的数据部分最好包括一客户机档案文件 270，它提供客户机档案信息并可从客户机 10 通过网络中介体 14 传送给服务器 18。最好是客户机档案文件 270 的至少一部分在从客户机 10 向网络中介体 14 传送时被加密。

尽管是例如参考单独的客户机档案模块 260 来说明本发明的，但本领域技术人员将会理解，客户机档案模块 260 还可以被纳入操作系统 252。这样，本发明不应被认作是限定于图 3 的配置，而是要包括能实现这里所述操作的任何配置。

现在将参考图 4 和图 5 更详细地描述本发明的实施例，图 4 和图 5 是根据本发明的实施例由客户机 10 和网络中介体 14 进行的操作的

流程图示例. 如图 4 中所见，客户机 10 产生一个客户机档案文件（块 100）. 客户机档案文件可以与一 HTTP 请求一起传送，可以是任何被同意的格式. 例如，客户机档案文件可以是一个 cookie、一个超文本置标语言（HTML）文件，扩展的置标语言（XML）文件，或其他这类语言的文件，或者它可以是具有任何适当的预先定义的格式的文件. 特定客户机档案文件的格式可能依赖于服务器 18 所期望的格式。尽管在这里把客户机档案描述为“文件”，但如本领域技术人员将会理解的那样，这里的“文件”是用于指客户机 10 向服务器 18 发送的档案信息的集合.

如图 4 中还可看到的那样，客户机 10 把指示器纳入客户机档案文件，该指示器指示要由网络中介体提供的信息（块 102）. 纳入客户机档案文件中的这个指示器授权由该指示器指定的特定特性要由网络中介体 14 提供，如代理服务器、网关服务器或服务提供器. 作为一例，该指示器可以包括通配符标识、如“$ OPEN”，它指定相关联的特性要由网络中介体 14 提供. 在这类实施例中，客户机档案文件可以包括下列内容:

```
…
<rdf:Description>
<prf:BearerNetwork> SMS</prf:BearerNetwork>
<prf:Bandwidth>9600</prf:Bandwidth>
<prf:Location>$OPEN</prf:Location>
</rdf:Description>
```

…通配符 $ OPEN 指定位置信息可能由网络中介体 14 提供.

如上文所见，客户机档案文件最好包括一个档案信息标识作为指示器的一部分，它标识要由网络中介体 14 提供的信息. 例如，在上例中的<prf:Location>…</prf:Location>序列提供一个标识，即位置信息是要由网络中介体提供的.

尽管在客户机档案文件中纳入指示器可以指定由网络中介体提供什么信息，但仅仅提供指示器可能会允许由假装客户机的某人进行不

适当的授权，并授权一网络中介体把关于该客户机的信息纳入客户机档案文件．然而，如图 4 中所见，该指示器可由客户机 10 加密（块 104），于是带有加密指示器的客户机档案文件被传送到服务器（块 106）．通过对指示器加密，客户机可以对指示器“签名”，从而能向网络中介体保证，是由该客户机产生的请求，要由网络中介体把信息纳入该档案．这样，可以缓解非授权用户从网络中介体得到客户档案信息的问题．

本发明的不同实施例可以以不同的方式对指示器加密．例如，在一个实施例中，客户机用它自己的私人密钥对通配符“$ OPEN”签字．再有，该通配符可以由“$ OPEN”加以改变，以包括客户机信息和/或随机产生的信息．例如，该通配符可采取如下形式:

<OPEN ID=“Client ID” Random=“12391321” >[VAL]</OPEN>

这里 ID 是客户机标识，Random 是一随机产生的令牌，[VAL]包含用客户机私人密钥加密的随机产生的令牌．可选择的是，一个字符串可与该令牌结合供加密．例如，该令牌可与串“$ OPEN”连接起来，然后由客户机私人密钥加密．

在本发明的又一些实施例中，可对整个档案序列加密．这样，在上述例子中，<prf:Location>…</prf:Location>序列可被加密．这可防止某人通过例如改变所请求的客户机特性来以该请求进行破坏活动．还可以通过加密带来特性标识的令牌，来把所请求的特性纳入[VAL]中．例如，该令牌可与

<prf:Location> $ OPEN</prf:Location>

一起被加密．如本领域技术人员将会理解的那样，只有该标识的一部分需要加密．再有，可以利用各种其他加密和/或指示器格式，同时仍可从本发明的说明中受益．

在本发明的又一些实施例中，利用网络中介体 14 的公共密钥进一步对指示器（例如上文描述的<OPEN…>序列）加密，从而可由客户机指定要授权哪个网络中介体提供该客户机信息．这样，通过保证只有被授权的网络中介体可以知道什么属性被请求了，从而可以减小欺

诈的机会.

图 5 显示根据本发明的实施例一网络中介体 14 的操作. 如图 5 中所见, 网络中介体 14 通过例如接收一个含有客户机档案文件的 HTTP 请求, 来接收该客户机档案文件 (块 120). 然后, 网络中介体评估该客户机档案文件并对客户机档案文件的加密部分解密 (块 122). 如果该客户机档案文件的一些部分是以网络中介体 14 的公共密钥加密的, 则该网络中介体 14 首先用它的私人密钥对客户机档案文件中以其公共密钥加密的那些部分解密. 否则, 网络中介体 14 可以利用与客户机档案文件的<OPEN…>字段中指定的客户机相关联的公共密钥的复制品来对该字段的[VAL]部分解密.

如果解密成功, 而且该网络中介体能提供所请求的信息, 则网络中介体 14 把所请求的信息纳入该客户机档案文件 (块 124). 这种纳入可采取以指定所请求信息的字段替代<OPEN…>字段的形式. 可选择的是, 如果需要进一步的安全性, 则可对这一信息加密. 在任何情况中, 网络中介体 14 可以把修改后的客户机档案文件再传送到服务器 (块 126). 再有, 网络中介体 14 可对所收到的<OPEN…>字段归档, 从而能在日后证明纳入客户机档案信息是由该客户机授权的.

图 1 至图 5 的流程图和方框图说明了一种可能的实现所具有的结构、功能和操作, 该实现根据本发明提供对来自公共源的密码功能的访问. 在这方面, 流程图中的每一块代表一个模块、片断或代码部分, 它包含一个或多个可执行的指令以实现指定的逻辑功能. 还应该指出, 在某些其他方式的实现中, 这些块中标明的功能可以不按图中所示顺序发生. 例如, 根据所涉及的功能, 相继显示的两块可能在事实上被基本同时执行或者这两块有时反序执行. 这样, 尽管本发明被描述为首先产生客户机档案文件, 然后纳入指示器并对指示器加密, 但如本领域技术人员将会理解的那样, 产生、纳入和加密可以作为单一操作或一些操作的组合来实现. 因此, 本发明不应被认为是局限于分离的操作, 而应被认为是讲述这些操作的结果, 而不论产生这些结果的动作如何分割.

尽管本发明的描述是参考客户机不能得到的信息进行的，但本领域技术人员将会理解，借助本说明，可由网络中介体为其他理由而提供信息。例如，该信息可能是客户机可得到的，然而，该客户机连接的带宽可能使得由一网络中介体发送该信息会更有效。

再有，本发明的描述是参考 HTTP 请求进行的，然而，本发明可应用于任何协议，只要它具有一个中介数据处理系统，该系统可以代表客户机向服务器提供由一协议字段指定的信息，这样，本发明不应被认作是局限于这里详细描述的本发明的 HTTP 实施例。

在附图和说明中已披露了本发明的典型最佳实施例，虽然利用了特定的术语，但它们只是在一般性的和描述性的意义上使用的，并不是为了限定的目的，本发明的范围将在后面的权利要求中提出。

说 明 书 附 图

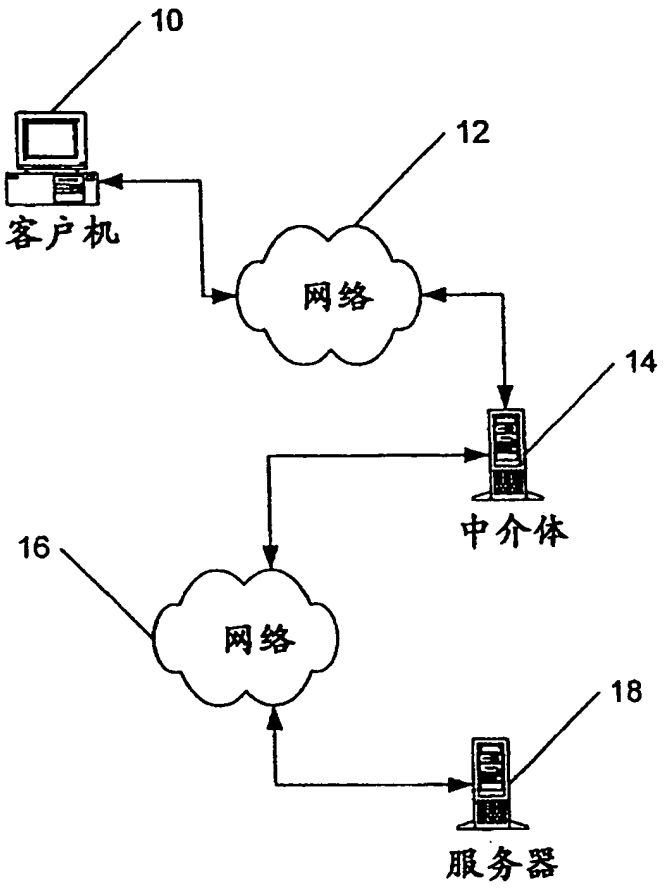


图1

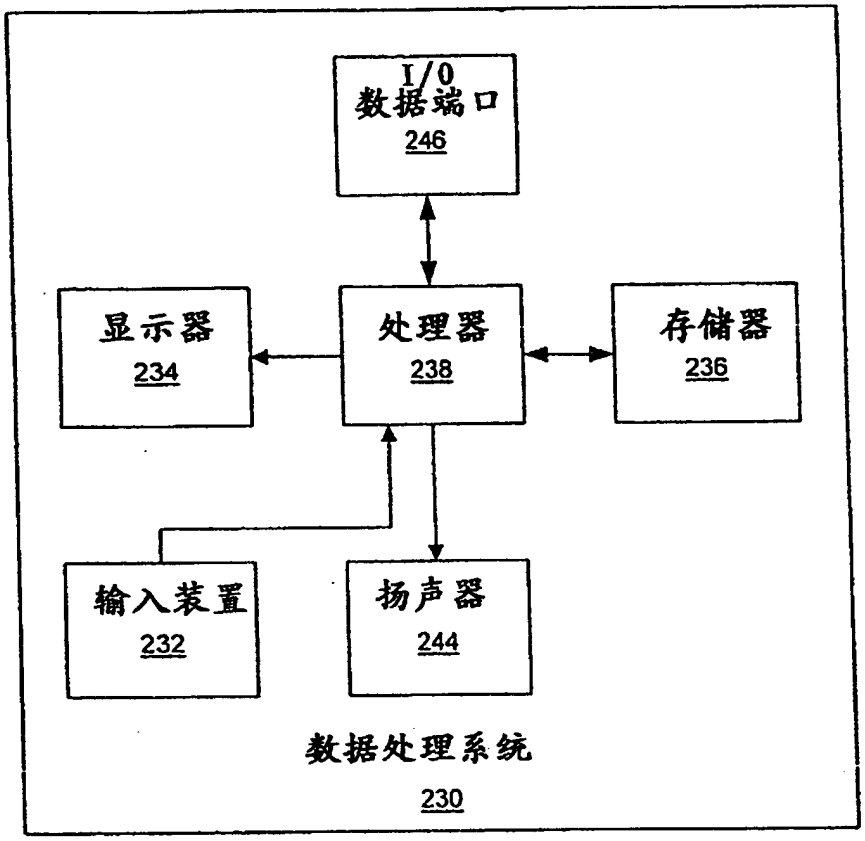


图2

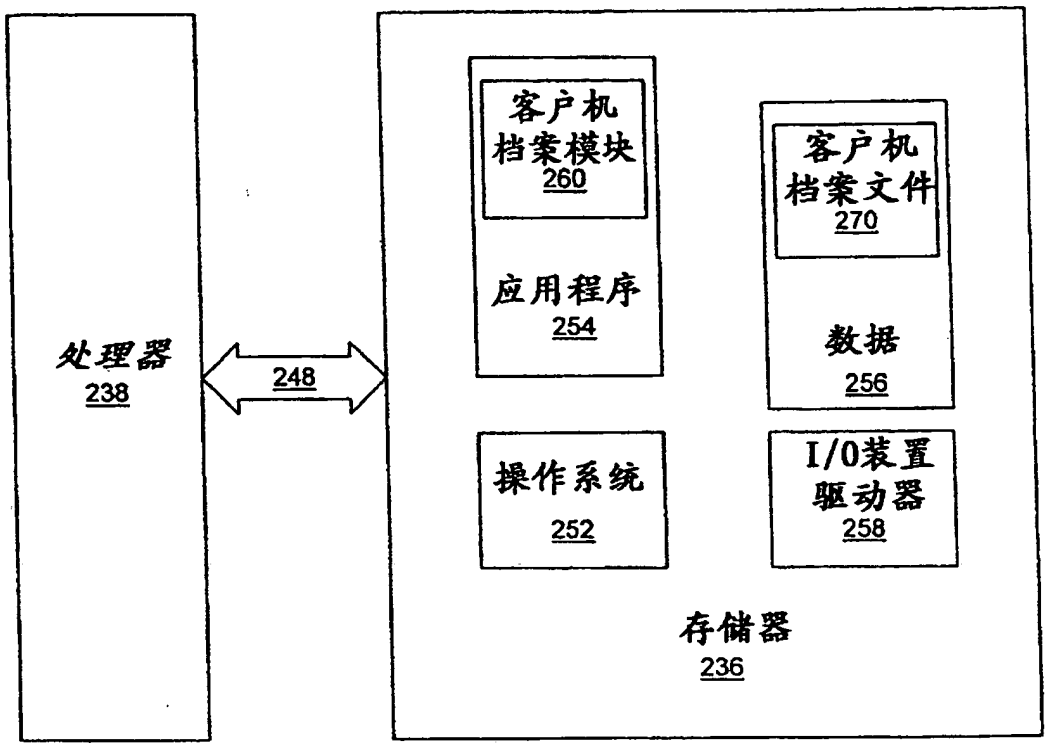

处理器
238
248
客户机
档案模块
260
应用程序
254
客户机
档案文件
270
数据
256
操作系统
252
I/O装置
驱动器
258
存储器
236

图 3

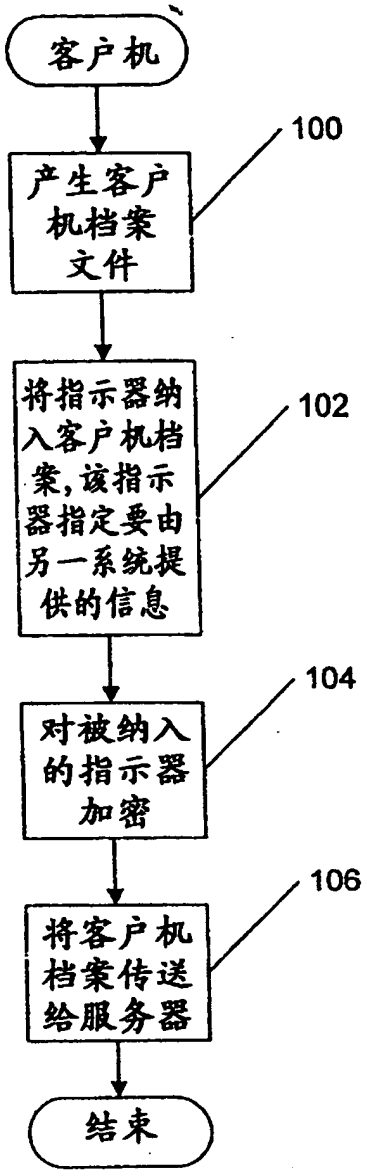

客户机
100
产生客户机档案文件
将指示器纳入客户机档案，该指示器指定要由另一系统提供的信息
102
对被纳入的指示器加密
104
将客户机档案传送给服务器
106
结束

图4

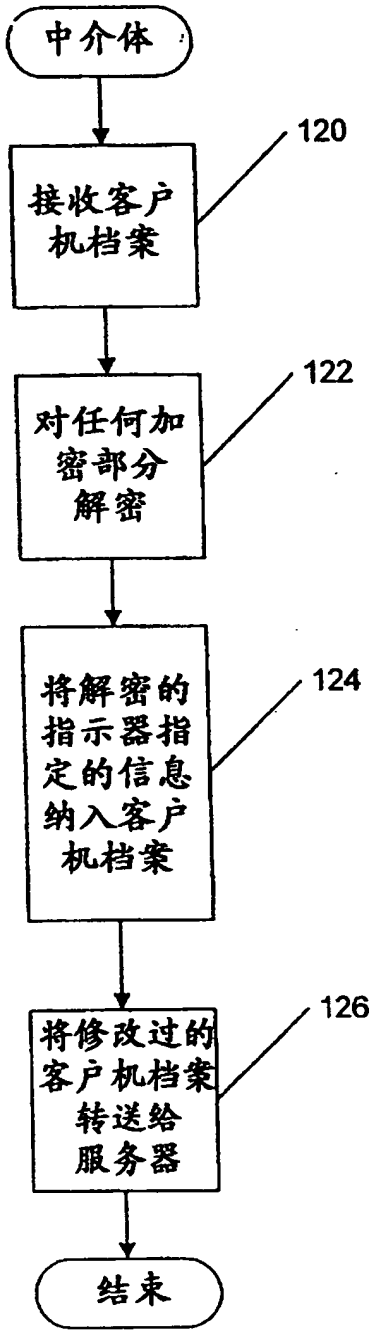

中介体
120
接收客户机档案
122
对任何加密部分解密
124
将解密的指示器指定的信息纳入客户机档案
126
将修改过的客户机档案转送给服务器
结束

图5

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☑ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.